Elementary Number Theory

Goal: Understand some basic properties of integers.

NB: $\mathbb{Z}$ = "set of integers"
$= \{\dots, -2, -1, 0, 1, 2, \dots\}$

Basic Properties of Arithmetic

$\mathbb{Z}$ comes with addition $+$ and multiplication $\cdot$.
These operations satisfy the following properties:

Let $a, b, c \in \mathbb{Z}$.

① $a+b \in \mathbb{Z}$ and $a \cdot b \in \mathbb{Z}$ (Closure)

② $a+b = b+a$ and $a \cdot b = b \cdot a$ (commutativity)

③ $a+(b+c) = (a+b)+c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (Associativity)

④ $a + (-a) = 0$ (negatives)

⑤ If $a \neq 0$, then $a \cdot \frac{1}{a} = 1$ (reciprocals)

↑ Not typically an integer...

⑥ $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ (Distributivity).

⑦ If $a \cdot b = 0$, then either $a = 0$ or $b = 0$.
→ Always refer to this by name... (Zero-product property).

(there are some order properties of real numbers...)

⑧ Either $a < b$ or $a > b$ or $a = b$ (Totally ordered).

→ ⑨ If $a \leq b$ and $c \geq 0$, then $ac \leq bc$.

⑩ If $a \leq b$, then $a + c \leq b + c$.

Defn: Let $m, n \in \mathbb{Z}$. We say m *divides* n (or m *is a factor of* n, or n *is a multiple of* m) when there is a $k \in \mathbb{Z}$ such that $n = m \cdot k$.

Notation: We write $m \mid n$ for the statement "m divides n".

Terminology: An integer is *even* when 2 divides it, and *odd* otherwise.

Ex: 6 is even b/c $6 = 2 \cdot 3$. ← $2 \mid 6 \equiv \exists_{k \in \mathbb{Z}} [6 = 2k]$

7 is odd b/c $2 \cdot 3 = 6 < 7 < 8 = 2 \cdot 4$.

NB: In formal predicate logic (when $m, n \in \mathbb{Z}$)

$$m \mid n := \exists_{k \in \mathbb{Z}} [n = mk].$$

Prop (Basic Properties of Divisibility):
Let $a, b, c \in \mathbb{Z}$. We have the following.

① Both $1 \mid a$ and $a \mid a$.

pf: Let $a \in \mathbb{Z}$ be arbitrary. Notice $a = 1 \cdot a = a \cdot 1$, so $1 \mid a$ and $a \mid a$ as desired. ☐

② If $a \mid b$, then both $-a \mid b$ and $a \mid -b$.

pf: Let $a, b \in \mathbb{Z}$ be arbitrary and assume $a \mid b$.

By definition of divisibility, there is an integer $k \in \mathbb{Z}$ such that $b = a \cdot k$. Now we may rewrite this as $b = a \cdot k = 1 \cdot a \cdot k = (-1)^2 ak = (-1 \cdot a) \cdot (-1 \cdot k) = (-a)(-k)$.

By closure under subtraction we observe $-a, -k \in \mathbb{Z}$.

Hence $b = (-a)m$ where $m = -k$ is an integer, so $-a \mid b$ by definition of divisibility. On the other hand $b = ak$ yields $-b = -(ak) = a(-k)$ by basic properties of arithmetic. Hence $m = -k \in \mathbb{Z}$ yields $a \mid -b$ by definition of divisibility.

Thus we conclude both $-a \mid b$ and $a \mid -b$ as desired ☑

③ If $a \mid b$ and $a \mid c$, then $a \mid (sb + tc)$ for all $s, t \in \mathbb{Z}$

pf: Let $a, b, c \in \mathbb{Z}$ be arbitrary and suppose $a \mid b$ and $a \mid c$. Let $s, t \in \mathbb{Z}$ be arbitrary. By definition of divisibility we have $b = ak$ and $c = am$ for some $k, m \in \mathbb{Z}$.

Aside

$(2 \mid 6) \wedge (2 \mid 8)$

$6 = 2 \cdot 3$, $3 = k$

$8 = 2 \cdot 4$, $4 = m$

Those k's are potentially different!

$(a \mid b) \wedge (a \mid c)$

$\equiv (\exists k_1 \in \mathbb{Z}\,[b = ak_1]) \wedge (\exists k_2 \in \mathbb{Z}\,[c = ak_2])$

Now we know

$sb + tc = s(ak) + t(am)$ (by substitution)

$= a(sk) + a(tm)$ (by comm and assoc of $\cdot$)

$= a(sk + tm)$ (by distributivity)

by basic arithmetic. On the other hand, $sk, tm \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under multiplication, and so $sk + tm \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under addition.

Hence $a \mid (sb + tc)$ by definition of divisibility. ☑

④ If $a|b$ and $b|c$, then $a|c$. (Transitivity of divisib.)

Pf: Let $a, b, c \in \mathbb{Z}$ be arbitrary, and assume $a|b$ and $b|c$. As $b|c$ we have $c = bk$ for some $k \in \mathbb{Z}$. As $a|b$ we have $b = am$ for some $m \in \mathbb{Z}$. Hence we have $c = bk = (am)k = a(mk)$. Moreover, $mk \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under multiplication. Hence $a|c$ by definition of divisibility. ☑

⑤ If $a, b > 0$ and $a|b$, then $a \leq b$.

Pf: Let $a, b \in \mathbb{Z}$ be arbitrary and assume $a, b > 0$ and $a|b$. As $a|b$, there is $k \in \mathbb{Z}$ such that $b = ak$. As $a, b > 0$, we have $k > 0$. Thus $k \geq 1$, so $a = a \cdot 1 \leq a \cdot k = b$ by order properties of the real numbers. Hence $a \leq b$ as desired. ☑

(NB Cor = Corollary = Statement w/ "easy" proof the previous result)

Cor: If $a|b$ and $b|a$, then $a = \pm b$.

Pf: Let $a, b \in \mathbb{Z}$ and assume $a|b$ and $b|a$. By part 2 of the preceding proposition, we may conclude both $|a| \,||\, |b|$ and $|b| \,||\, |a|$ (because $-a|b$ and $a|-b$ and $-b|a$ and $b|-a$ and $|a| = \pm a$ and $|b| = \pm b$) we proceed by cases on $|a|$.

Case 1: If $|a| = 0$, then $a = 0$. So $b = ak$ for some $k \in \mathbb{Z}$ yields $b = 0$, so $a = b$ as desired.

Case 2: If $|a| \neq 0$, then $a \neq 0$ so $|a| > 0$. Now $|b| = |a|k$ for some $k \in \mathbb{Z}$. If $k = 0$, then $|b| \mid |a|$ would again (similar to case 1) yield $a = b = 0$. but this would contradict $a \neq 0$. Hence $k \neq 0$.

How: Simplify this.

By order properties of $\mathbb{R}$ we have $k > 0$, hence $|b| > 0$ so we know both $|a|, |b| > 0$. By part 5 of the preceding proposition, we have $|a| \leq |b|$ because $|a| \mid |b|$, and $|b| \leq |a|$ because $|b| \mid |a|$; Hence $|a| = |b|$, so $a = \pm b$ as desired. ☒.